DIALOG(R)File 352:Derwent WPI

012735357 **Image available**
WPI Acc No: 1999-541474/199946
XRPX Acc No: N99-401334
Cashless financial transaction system with biometric entry device
Patent Assignee: HAMESTER U (HAME-I)
Inventor: HAMESTER U
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
DE 19809006	A1	19990909	DE 1009006	A	19980303	199946	B

Priority Applications (No Type Date): DE 1009006 A 19980303
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
DE 19809006	A1		5	G06F-017/60	

Abstract (Basic): DE 19809006 A1

NOVELTY - The cashless financial transaction system has a keyboard (1) with an integral identification system (3-7) for such as a smart card. In addition to the smart card code the system uses biometric data such as fingerprints, eye and speech characteristics. The data is fed to a central computer (9) and this provides access to various networks.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for a cashless transaction method.

USE - Banking systems

ADVANTAGE - Improved security

DESCRIPTION OF DRAWING(S) - Block diagram

Keyboard (1)

Identification system (3-7)

computer (9)

pp; 5 DwgNo 1/1

Title Terms: FINANCIAL; TRANSACTION; SYSTEM; ENTER; DEVICE
Derwent Class: S05; T01; T04; T05; W01
International Patent Class (Main): G06F-017/60
International Patent Class (Additional): G06F-019/00; G06K-009/62
File Segment: EPI

EP 21231 (6)

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 198 09 006 A 1**

(51) Int. Cl.[6]:
G 06 F 17/60
G 06 F 19/00
G 06 K 9/62

(21) Aktenzeichen: 198 09 006.4
(22) Anmeldetag: 3. 3. 98
(43) Offenlegungstag: 9. 9. 99

DE 198 09 006 A 1

(71) Anmelder:
Hamester, Uwe, Dipl.-Ing. (FH), 90513 Zirndorf, DE

(72) Erfinder:
gleich Anmelder

(56) Für die Beurteilung der Patentfähigkeit in Betracht zu ziehende Druckschriften:

DE	43 22 445 C1
DE	196 52 393 A1
DE	196 28 045 A1
DE	196 28 044 A1
DE	195 41 672 A1
DE	44 47 435 A1
DE	36 33 360 A1
EP	07 93 186 A2
EP	06 52 540 A1

ROTTMANN,Sigrun: Das Auge ersetzt die Geheimzahl. In: Berliner Zeitung, 08.07.1996, Nr.157, S.15;
Test: Geld nur mit "richtigem Gesicht", Münchner Merkur, Nr.63, 17.03.98, Wirtschaftsteil;
Voice Recognition with Non-Audio Sensor. In: IBM Technical Disclosure Bulletin, Vol.40, No.04, April 1997, S.5,6;

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Der Inhalt dieser Schrift weicht von den am Anmeldetag eingereichten Unterlagen ab

(54) Zahlungssystem mit biometrischen Eingabevorrichtungen

(57) Die vorliegende Erfindung stellt ein Zahlungssystem und -verfahren mit wesentlichen Vorteilen im bargeldlosen Zahlungsverkehr bereit. Dazu wird erfindungsgemäß vorzugsweise ein biometrisches Erkennungssystem zur Authentisierung und Autorisierung von Benutzern verwendet. Die Transaktionsdaten werden über ein weltweites Netzwerk mit einem Rechenzentrum übermittelt.

DE 198 09 006 A 1

Beschreibung

Die vorliegende Erfindung betrifft ein Zahlungssystem und -verfahren mit biometrischen Eingabevorrichtungen.

Bei bargeldlosen Zahlungssystemen spielt einerseits die Sicherheit und andererseits die einfache Verfügbarkeit und Funktionsweise eine wesentliche Rolle. Die derzeit bekannten und herkömmlichen bargeldlosen Zahlungssysteme werden den Anforderungen nur unzureichend gerecht.

Es liegt der vorliegenden Erfindung daher die Aufgabe zugrunde, ein verbessertes bargeldloses Zahlungssystem und -verfahren zur Verfügung zu stellen. Insbesondere ist es eine Aufgabe der Erfindung, den Mißbrauch von bargeldlosen Zahlungssystemen zu minimieren und Partnern, wie Kunden, ein einfach handhabbares, sicheres und flexibles bargeldloses Zahlungssystem zur Verfügung zu stellen. Diese Aufgabe wird mit den Merkinalen der Patentansprüche gelöst.

Für das erfindungsgemäße Verfahren bzw. System können diverse Eingabesysteme zum Einsatz kommen. Zum Beispiel kann eine Tastatur oder ein Notepad verwendet werden.

Bei der Tastatur handelt es sich vorzugsweise um eine Zehnertastatur mit ergänzenden Tasten, wie sie bei heute üblichen Kreditkartenlesern im Einsatz ist. Je nach verwendetem Erkennungssystem sind weitere Steuertasten notwendig.

Bei dem Notepad handelt es sich vorzugsweise um ein Eingabesystem, das mit einem Stift oder mit den Fingern bedient wird und sowohl Eingaben, als auch Anzeigen auf einem Feld zuläßt. Dadurch ist eine flexible Gestaltung der Eingabemöglichkeiten ohne Anpassung des physikalischen Eingabesystems möglich. Diese Technik ist heute in sogenannten Palmtop-Rechnern im Einsatz, die häufig zur elektronischen Terminplanung dienen.

Ferner können diverse Erkennungssysteme zum Einsatz kommen, wie z. B. ein Kartenleser mit "intelligenter" Karte (smart card), (Lebend-)Finger-Erkennungssystem/Hautpartie-Erkennungssystem, (Lebend-)Gesichts-Erkennungssystem, (Lebend-)Augen-Erkennungssystem und/oder (Lebend-)Sprach-Erkennungssystem.

Bei Kartenlesern mit "intelligenter" Karte (smart card) ist auf der Karte so viel "Intelligenz" integriert, daß die Karte selbständig den Verbindungsaufbau mit einer eindeutigen Autorisierung, Authentisierung und einem gesicherten, verschlüsselten Zahlungsverkehr durchführt.

Bei einem (Lebend-)Finger-Erkennungssystem/Hautpartie-Erkennungssystem handelt es sich vorzugsweise um ein Finger-Erkennungssystem, wie es heute bei Zugangssystemen für zugangsgeschützte Räumlichkeiten zum Einsatz kommt. Es können auch beliebige andere Hautpartien (z. B. Unterarm) zur Erkennung herangezogen werden. Durch Vergleich des eingelesenen Hautmusters mit einem in einem vorzugsweise verteilten Rechenzentrum gespeicherten Original-Hautmuster wird die eindeutige, fälschungssichere Erkennung des Originals durchgeführt.

Durch zusätzliche Maßnahmen, wie Messung der Hauttemperatur, Pulsschlag etc. kann die Lebendigkeit eines Fingers bzw. einer Hautpartie überprüft werden. Ein lebloses (= künstliches) bzw. abgetrenntes Organ wird nicht mehr als Original-Hautmuster erkannt. Der Zahlungsvorgang wird in einem solchen Fall nicht durchgeführt.

Bei einem (Lebend-)Gesichts-Erkennungssystem wird vorzugsweise mit einer Kamera z. B. das Gesicht einer Person aufgenommen. Durch Vergleich des eingelesenen Gesichtes mit der/den in einem z. B. verteilten Rechenzentrum gespeicherten Original-Gesichtsaufnahme(n) wird eine eindeutige, fälschungssichere Erkennung des Originals durchgeführt.

Durch Bewegungen von Gesichtszügen, wie z. B. Lächeln, Zwinkern mit den Augen etc., kann das Gesicht auf Lebendigkeit überprüft werden. Ein Bild oder ein regungsloses Gesicht, wie z. B. eine Maske, wird dann nicht mehr als Original erkannt. Der Zahlungsvorgang wird somit nicht durchgeführt.

Ein (Lebend-)Augen-Erkennungssystem tastet mit einer Abtasteinheit (z. B. Laser) die Struktur eines Auges ab. Durch Vergleich des abgetasteten Auges mit einer in einem vorzugsweise verteilten Rechenzentrum gespeicherten Original-Augenstruktur wird die eindeutige, fälschungssichere Erkennung des Originals durchgeführt.

Durch Bewegungen, z. B. der Pupille, bzw. durch zusätzliche Maßnahmen, wie Messung der Augentemperatur etc., kann das Auge auf Lebendigkeit überprüft werden. Ein Bild oder ein regungsloses, z. B. künstliches Auge wird somit nicht mehr als Original erkannt. Der Zahlungsvorgang wird in diesem Fall nicht durchgeführt.

Bei einem (Lebend-)Sprach-Erkennungssystem mit einem Mikrofon wird die Stimme aufgenommen. Durch Vergleich der aufgenommenen Stimme mit einer in einem vorzugsweise verteilten Rechenzentrum gespeicherten Original-Stimme wird die eindeutige, fälschungssichere Erkennung des Originals durchgeführt. Störende Nebengeräusche werden vorzugsweise vom Vergleichssystem im wesentlichen ausgefiltert.

Durch Aufforderung bestimmte, z. B. stets wechselnde Worte zu sagen, kann die Stimme auf Lebendigkeit überprüft werden. Eine Tonaufzeichnung oder eine verstellte Stimme etc. wird dann nicht mehr als Original erkannt. Der Zahlungsvorgang wird somit nicht durchgeführt.

Das erfindungsgemäße System bzw. Verfahren verwendet vorzugsweise z. B. eine Zahlungsvorrichtung, die eine Kombination aus einem oder mehreren Eingabesystemen und einem oder mehreren Erkennungssystemen ist. Die Zahlungsvorrichtung dient zur Authentisierung des Kunden (=Person, die das beschriebene Zahlungssystem zur Zahlung nutzt).

Alle Zahlungsvorrichtungen werden vorzugsweise mit einem Chip oder anderen Speichermedium (z. B. Magnetstreifen) konstruiert, der oder das beim Verbindungsaufbau mit Hilfe des sog. Kerberos-Protokolles eine eindeutige Autorisierung und Authentisierung der Zahlungsvorrichtung durchführt. Alle daran anschließenden Datenübertragungen werden bevorzugt voll verschlüsselt. Der Chip ist so mit dem jeweiligen Erkennungssystem verbunden, daß er eine nicht trennbare und nicht abgreifbare Einheit bildet. Wird versucht, diese Einheit zu trennen bzw. dazwischen die Signale abzugreifen, so kann sich der Chip, z. B. selbständig zerstören, so daß weder Nachbau noch Manipulation möglich sind. Nach dem gesicherten, verschlüsselten Übertragen des Datenstromes wird der Zahlungsverkehr im Rechenzentrum nach einer Autorisierungsprüfung des Kunden angestoßen. Der verwendete Schlüssel liegt auf dem Chip gespeichert und wird automatisch bei jeder Transaktion geändert. Beim Kartenleser ist der Chip in die Karte integriert.

Ferner ist eine Zahlungseinheit vorgesehen, die zur Authentisierung des Partners dient, z. B. eine Firma, die die Zahlung über das beschriebene Zahlungssystem anbietet. Die Zentraleinheit ist mit einem Chip konstruiert, der beim Verbindungsaufbau mit Hilfe des Kerberos-Protokolles eine eindeutige Autorisierung und Authentisierung der Zentraleinheit und somit des Partners durchführt. Alle daran anschließenden Datenübertragungen werden vorzugsweise voll verschlüsselt. Der verwendete Schlüssel liegt auf dem Chip gespeichert und wird z. B. automatisch bei jeder Transaktion geändert.

Der Datenstrom der Zahlungsvorrichtung wird so in den Datenstrom der Zentraleinheit integriert, daß im Rechenzentrum die eindeutige Zuordnung von Kunde und Partner erfolgen kann. Bei Zahlungen über z. B. das Internet steht die Zahlungsvorrichtung an einem beliebigen anderen Ort und hat keinen direkten Bezug zur Zentraleinheit. Durch das verwendete Integrationsverfahren der Datenströme wird online die eindeutige Zuordnung von Kunde (Zahlungsvorrichtung) und Partner (Zentraleinheit) im Rechenzentrum sichergestellt.

Das erfindungsgemäße Verfahren und System weist z. B. mindestens ein Kompaktgerät auf. Das Kompaktgerät ist eine Vorrichtung, in der vorzugsweise die Zahlungsvorrichtung und Zentraleinheit in einer Vorrichtung direkt verbunden sind. Es ist jeweils ein Eingabesystem, ein oder mehrere Erkennungssysteme und eine Zentraleinheit dazu vorgesehen. Das Kompaktgerät wird z. B. direkt mit dem weltweiten Netz (z. B. Internet, Intranet usw.) verbunden.

Unter Verwendung einer Mehrgerätekonfiguration bzw. -vorrichtung können Zahlungstransfers mehrerer Zahlungsvorrichtungen über eine Zentraleinheit folgen. Dabei werden vorzugsweise die Zahlungsvorrichtungen mit Kabel, einer funkgebundenen Inhausdatenübertragung (z. B. DECT-Technik) oder einer funkgebundenen Weitverkehrsdatenübertragung (z. B. GSM-Technik) mit der Zentraleinheit verbunden.

Die Inhausdatenübertragung zwischen Zahlungsvorrichtung und Zentraleinheit erfolgt über Kabel oder Funk (wie bei schnurlosen Telefonen) mit analoger Technik oder mit digitaler DECT-Technik. Dabei kann eine Entfernung bis zu ca. 300 Meter überwunden werden.

Beim externen Einsatz von Zahlungsvorrichtungen mit einer funkgebundenen Weitverkehrsdatenübertragung zwischen Zahlungsvorrichtung und Zentraleinheit wird, z. B. die vom Handy bekannte Technik (z. B. GSM) eingesetzt. Damit ist es möglich, beliebig weit von der Zentraleinheit entfernt mit mobilen Zahlungsvorrichtungen zu arbeiten.

Bei einer Benutzung des weltweiten Netzes kann die Übertragung der Daten z. B. über das Internet, Intranet, über dedizierte Leitungen, über das bei heutigen Zahlungssystemen eingesetzte Netz zwischen Zentraleinheit und verteiltem Rechenzentrum oder sonstige drahtlose oder drahtgebundene Übertragungselemente erfolgen.

Das für die vorliegende Erfindung vorzugsweise benutzte verteilte Rechenzentrum ist an geeigneten Standorten über die Erde verteilt. Es liefert den Partnern (Firmen, die Zahlung über das beschriebene Zahlungssystem anbieten) und Kunden (Personen, die das beschriebene Zahlungssystem nutzen) die erforderlichen Dienste in der Nähe ihrer Standorte.

Durch das erfindungsgemäße System und Verfahren werden insbesondere die folgenden Vorteile erzielt, daß ein direkter Anstoß des Zahlungsvorgangs durch ein biometrisches und/oder herkömmliches Erkennungsmedium, wie eine smart card erfolgt, ein flexibler Einsatz der Zahlungsvorrichtungen durch kabel- oder funkgebundene Datenübertragung möglich ist, und die Übertragung zum abrechnenden, verteilten Rechenzentrum über unterschiedliche, weltweite Netze erfolgen kann. Da die gesamte Transaktion immer voll verschlüsselt durchgeführt wird, können auch relativ "unsichere" Netze, wie z. B. das Internet, zur Übertragung genutzt werden. Ein weiterer Vorteil ist gerade bei Einsatz von mehreren Zahlungsvorrichtungen in einem Haus bzw. an verschiedenen Orten, daß mit nur einem Anschluß an das weltweite Netz gearbeitet werden kann, da die Zentraleinheit die Eingabe- und Erkennungssysteme simultan bedienen kann. Man spart dadurch Leitungskosten und Anschlußgebühren. Alternativ kann, wie bei herkömmlichen Zahlungssystemen, auch jede Zahlungsvorrichtung direkt über ein Kompaktgerät an ein weltweites Netzwerk angeschlossen werden. Weitere Vorteile sind z. B. daß ein Kunde kein Bargeld bei sich haben muß, das ihm möglicherweise geraubt oder gestohlen werden kann, ein Partner sich auf den Zahlungseingang verlassen kann, sobald die Transaktion abgeschlossen ist, da der Zahlungsvorgang online durchgeführt wird, Kunde wie Partner sicher sein können, daß ein Mißbrauch des Zahlungssystems nahezu ausgeschlossen ist, da die biometrischen Merkmale nach heutigem Wissen fälschungssicher sind und die "intelligente" Karte den heute üblichen Sicherheitsstandard von Kreditkarten etc. deutlich verbessern kann. Das bloße Wissen der Kartennummer reicht nicht aus, um Abbuchungen vorzunehmen.

Der Datenstrom kann jederzeit bei der Übertragung zwischen Zahlungsvorrichtung und dem Rechenzentrum mitgeschnitten werden. Durch die voll verschlüsselte Übertragung kann der Schlüssel selbst, wenn überhaupt, nur mit sehr aufwendigen Entschlüsselungsverfahren entschlüsselt werden. Da sich der Schlüssel in kürzeren Zeitabständen ändert als die zu einer möglichen Entschlüsselung erforderliche Zeitdauer ist, kann der gerade aktuelle Schlüssel nie zum Zeitpunkt seiner Gültigkeit verwendet werden. Das System ist somit völlig abhörsicher.

Vorteilhaft ist ferner, daß ein Reisender bei Zahlungen seiner Kunden kein Bargeld mit sich führen muß, der Verlust einer funkgebundenen Zahlungsvorrichtung keinen Mißbrauch ermöglicht, da die Zahlungen, die möglicherweise damit angestoßen werden, immer nur auf das Konto des Partners gelangen können. Der Versuch, die Zahlungsvorrichtung zu manipulieren, führt zu deren Zerstörung. Weitere positive Effekte des erfindungsgemäßen Verfahrens und Systems sind, daß das Eingabefeld gleichzeitig die Anzeige darstellt und bei geschickter Gestaltung der Anzeige eine intuitive Bedienung ermöglicht wird, das Eingabefeld und die Anzeige an neue Bedürfnisse leicht angepaßt werden können, flexible Zahlungsweisen mit unterschiedlichen biometrischen Merkmalen (Finger/Haut, Gesicht, Auge, Sprache) ermöglicht werden, ein Kunde kein Bargeld und keine Karte dabei haben muß, um bezahlen zu können, z. B. ein Reisender jederzeit Zahlungen über eine funkgebundene Zahlungsvorrichtung entgegennehmen kann, das Entleeren von Automaten durch eine online Buchung entfällt.

Die Erfindung wird im folgenden anhand einer bevorzugten Ausführungsform beispielhaft beschrieben. Es zeigt:

Fig. 1 eine schematische Darstellung eines erfindungsgemäßen bargeldlosen Zahlungssystems.

Das erfindungsgemäße bargeldlose Zahlungssystem weist verschiedene, modular miteinander kombinierbare Eingabesysteme, wie z. B. eine Tastatur **1** oder ein Eingabepad (Notepad) **2** oder Erkennungssysteme **3–7** auf. Die Erkennungssysteme sind vorzugsweise ein Kartenleser mit "intelligenter" Karte (smart card) **3**, ein (Lebend-)Finger-Erkennungssystem und/oder Hautpartie-Erkennungssystem **4**, ein (Lebend-)Gesichts-Erkennungssystem **3**, ein (Lebend-)Augen-Erkennungssystem **6** und/oder ein (Lebend-)Sprach-Erkennungssystem **7**. Die Eingabe- und Erkennungssysteme **1–7** sind vorzugsweise in einer Zahlungsvorrichtung **8** zu einem Kompaktgerät zusammengefaßt. Die Zahlungsvorrichtung **8** bildet vorzugsweise zusammen mit einer Zentraleinheit **9** eine Mehrgerätekonfiguration **11**.

Die Zahlungsvorrichtung **8** dient zur Authentisierung des Kunden, d. h. der Person, die das beschriebene Zahlungssystem zur Zahlung nutzt. Die Zentraleinheit **9** dient zur Authentisierung des Partners, d. h. der Person oder Firma, die die Zahlung über das beschriebene Zahlungssystem anbietet.

Die Zahlungsvorrichtung **8** ist eine Vorrichtung, in der das mindestens eine Eingabesystem **1** oder **2**, das mindestens eine Erkennungssystem **3–7** und die Zentraleinheit **9** in einer Vorrichtung, nämlich der Mehrgerätekonfiguration **11** direkt verbunden sind.

Die Mehrgerätekonfiguration **11** ist eine Vorrichtung, die Zahlungstransfers mehrerer Zahlungsvorrichtungen **8** über eine Zentraleinheit **9** ermöglicht, während dabei die Zahlungsvorrichtungen **8** mit Kabel, einer funkgebundenen in Hausdatenübertragung (z. B. DECT-Technik) oder einer funkgebundenen Weitverkehrsdatenübertragung (z. B. GSM-Techhik) mit der Zentraleinheit **9** verbunden sind.

Kompaktgeräte **12** sind mit der oder den Mehrgeräte-Konfiguration(en) über einen direkten Anschluß an ein weltweites Netz **13** zur Übertragung der Zahlungsdaten an ein evtl. weltweit verteiltes Rechenzentrum **14** angebunden. Über das Rechenzentrum **13** werden Transaktionen, z. B. Abbuchungen, Gutschriften u.ä., abgewickelt.

Das Kompaktgerät **12** ist vorzugsweise wiederum eine Zahlungsvorrichtung mit integrierter Zentraleinheit, wie vorstehend bereits beschrieben. Beliebig viele weitere Kompaktgeräte **12** gegebenenfalls können an das Netzwerk **13** oder andere Netzwerke oder Übertragungsmedien angeschlossen werden.

Patentansprüche

1. System zur bargeldlosen Zahlung mit:
mindestens einer Mehrgerätekonfiguration (**11**), die mindestens ein Eingabesystem (**1, 2**) und mindestens ein damit modular kombinierbares Erkennungssystem (**3–7**) aufweist, um eine Zahlungsvorrichtung (**8**) zu bilden, und die ferner eine Zentraleinheit (**9**) aufweist, die mit der Zahlungsvorrichtung (**8**) in Verbindung steht, wobei die Zahlungsvorrichtung (**8**) zur Authentisierung eines Benutzers und die Zentraleinheit (**9**) zur Authentisierung eines Partners dient, das Eingabesystem (**1, 2**), das Erkennungssystem (**3–7**) und die Zentraleinheit (**9**) in der Mehrgerätekonfiguration (**11**) direkt miteinander verbunden sind, und die Mehrgerätekonfiguration (**11**) eine Vorrichtung ist, die Zahlungstransfers mehrerer Zahlungsvorrichtungen über mindestens eine Zentraleinheit (**9**) ermöglicht;
einer Anschlußvorrichtung für den Anschluß an ein Netzwerk (**13**), das zur weltweiten Datenübertragung geeignet ist; und
einem Rechenzentrum (**14**), über das Transaktionen abgewickelt werden, wobei das Rechenzentrum (**14**) mit dem Netzwerk (**13**) in Verbindung steht.

2. System nach Anspruch 1, wobei die Zahlungsvorrichtungen (**8**) über Kabel, einer funkgebundenen Inhausdatenübertragung und/oder einer funkgebundenen Weitverkehrsdatenübertragung mit der Zentraleinheit (**9**) in Verbindung stehen.

3. System nach Anspruch 1 oder 2, wobei zur eindeutigen Autorisierung und/oder Authentisierung mindestens ein biometrisches Erkennungssystem vorgesehen ist.

4. System nach einem der Ansprüche 1 bis 3, wobei das Eingabesystem eine Tastatur (**1**) und/oder ein Notepad (**2**) ist.

5. System nach Anspruch 4, wobei das Notepad (**2**) so ausgebildet ist, daß es gleichzeitig als Anzeigesystem verwendbar ist.

6. System nach einem der Ansprüche 1 bis 5, wobei das Netzwerk (**13**) ein Telefonnetz, das Internet, ein privates Netz und/oder ein Banknetz ist.

7. Verfahren zur bargeldlosen Zahlung mit den Schritten:
a) Eingeben einer geplanten Transaktion mit einem Eingabesystem (**1, 2**);
b) Überprüfen der Befugnis des Benutzers für die Transaktion mittels eines Erkennungssystems (**3–7**);
c) Übertragen der Transaktionsdaten an eine Zentraleinheit (**9**); und
d) Senden der Transaktionsdaten von der Zentraleinheit (**9**) über ein Netzwerk (**13**) mit einem damit verbundenen Rechenzentrum (**14**) an einen Empfänger.

8. Verfahren nach Anspruch 7, wobei die Datenübertragung zwischen der Zahlungsvorrichtung (**8**) und der Zentraleinheit (**9**) über Kabel-, funkgebundene Inhaus- oder funkgebundene Weitverkehrsdatenübertragung erfolgt.

9. Verfahren nach Anspruch 7 oder 8, wobei das Erkennungssystem (**3–7**) zur eindeutigen Autorisierung und/oder Authentisierung biometrische Erkennungssysteme verwendet.

Hierzu 1 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 198 09 006 A1
Int. Cl.[6]: G 06 F 17/60
Offenlegungstag: 9. September 1999

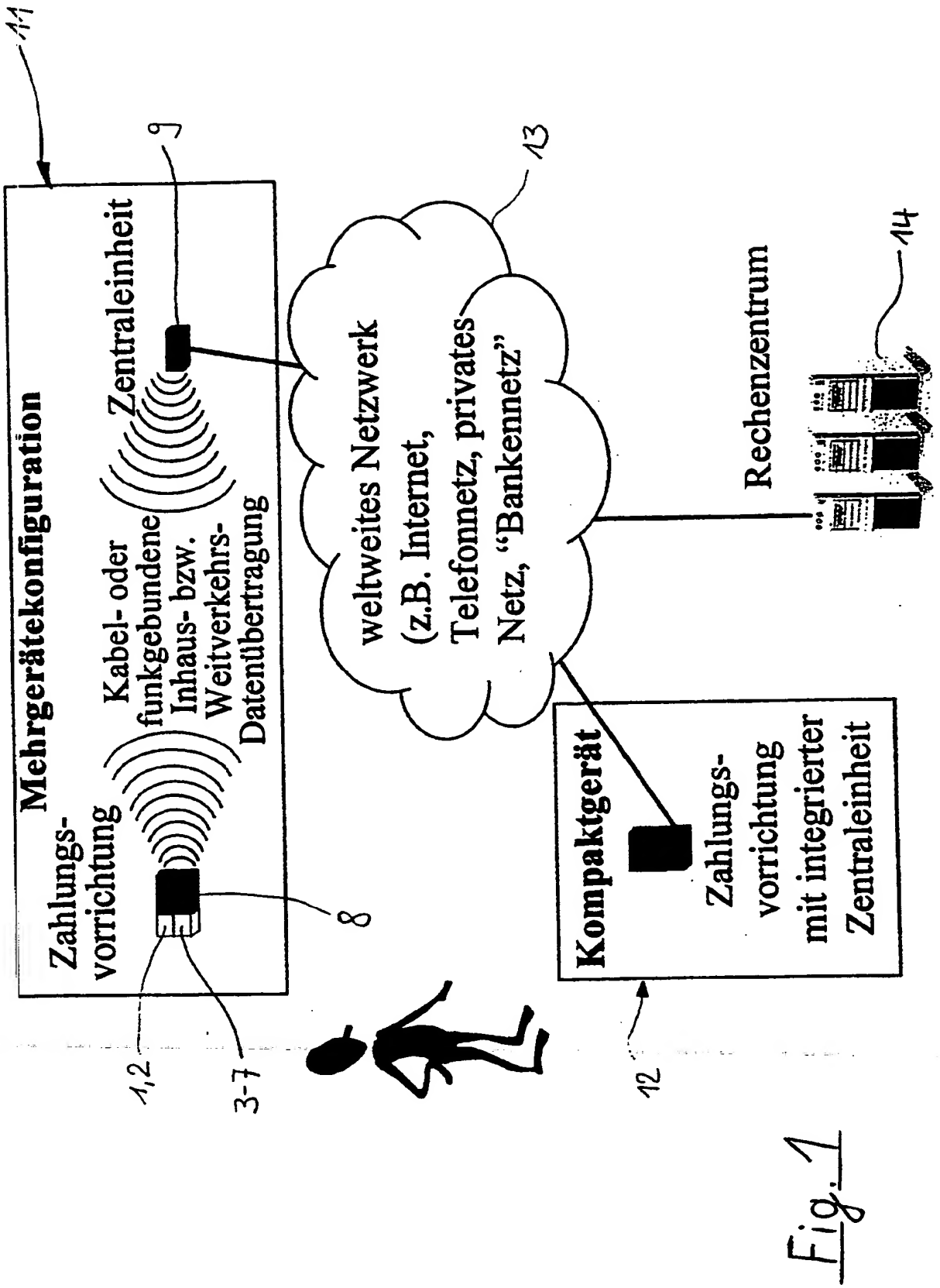

Fig. 1